

FIG. 2

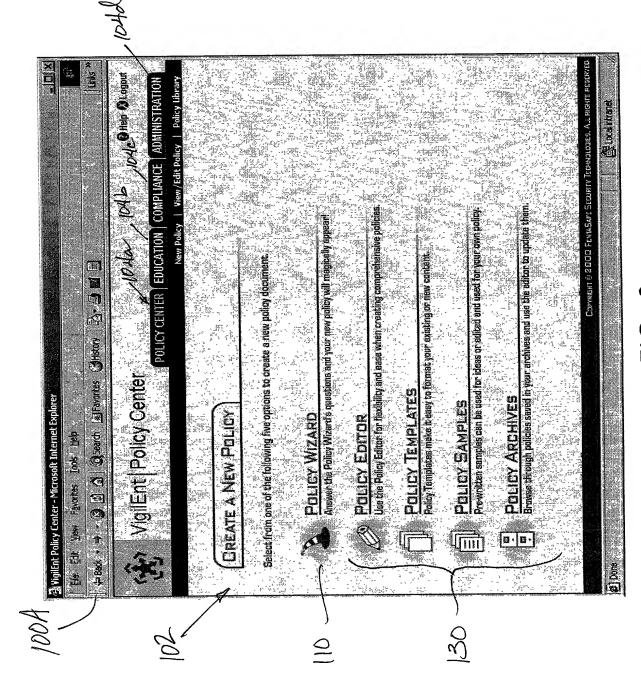
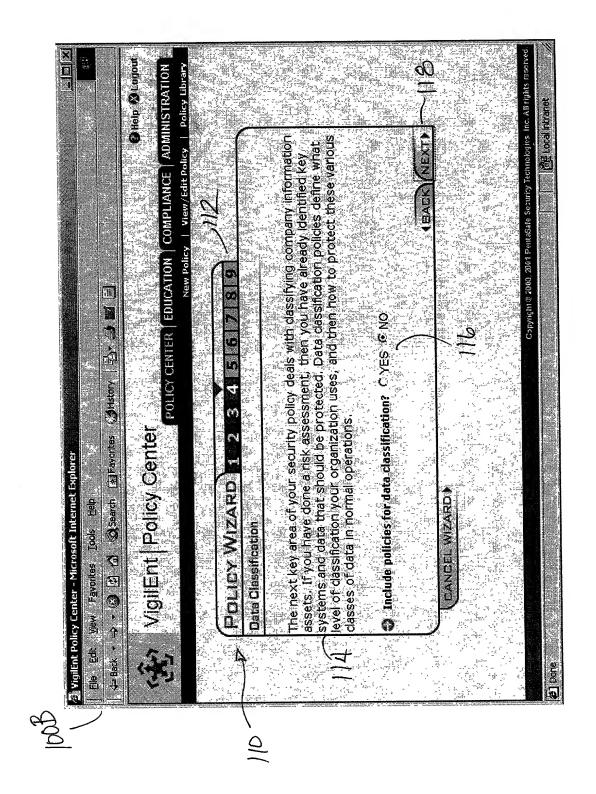


FIG. 3



FIG, 4A

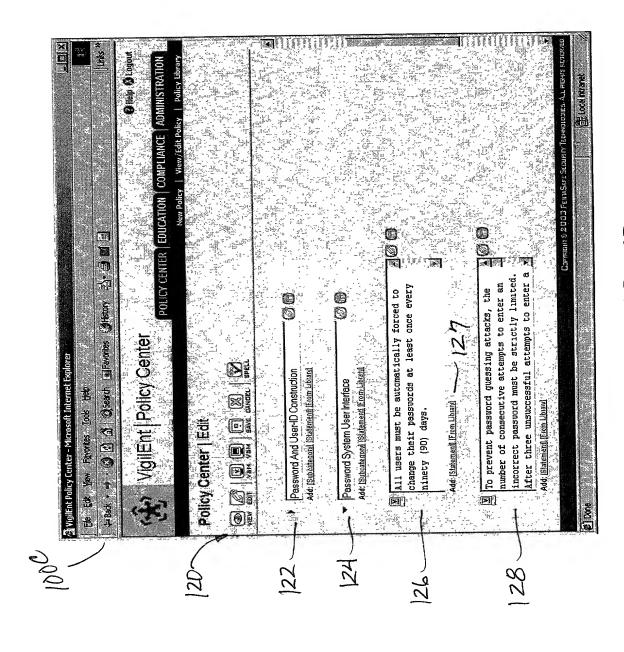


FIG. 4B

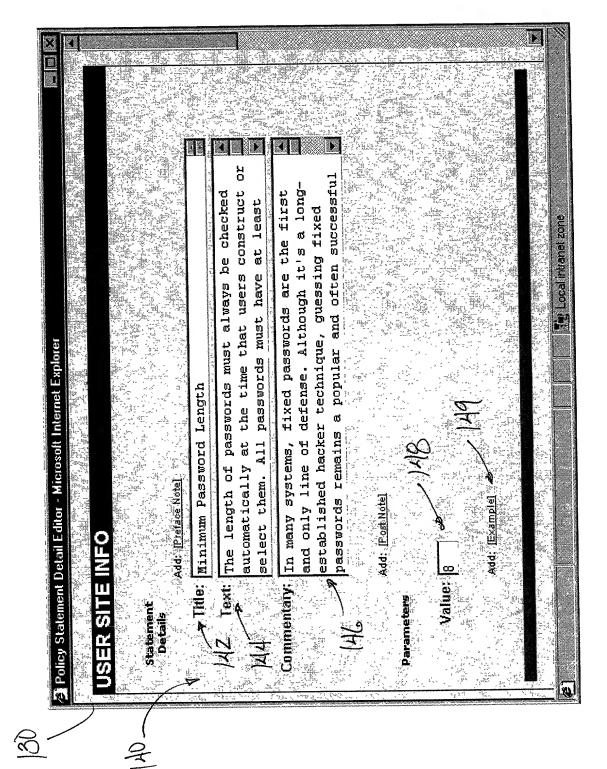


FIG. 5A

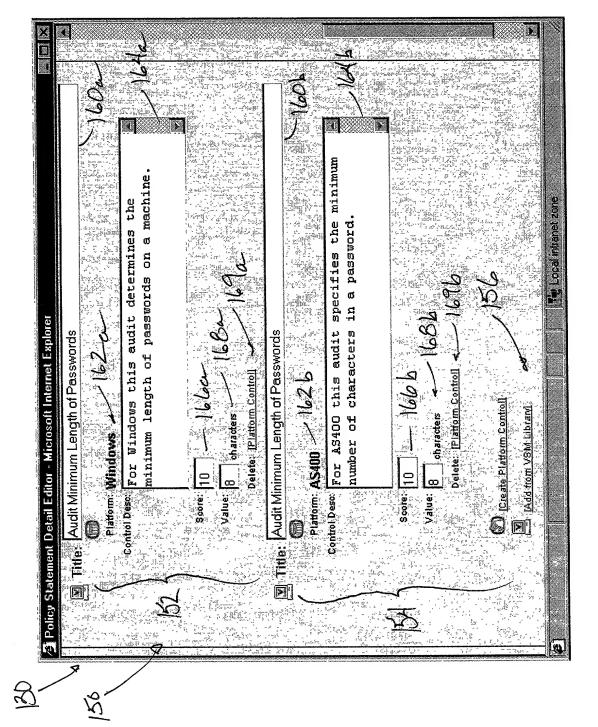


FIG. 5B

203u <POLICY DOCUMENT title="AS400 Policy For VSM" createDate="2000-05-18" updateDate="2000-08-25" author="Dave Lineman" docType="Policy Document Library" docState="System"> <POLICY CATEGORY title="Password Management" orderValue="0"> <POLICY STATEMENT identifier="CW_PD_MINLEN" name="Minimum"</pre> Password Length" categoryOrder="0" printFormat="0" agentIdentifier="VSM"> <POLICY STATEMENT TEXT>The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least eight (8) characters.</POLICY STATEMENT TEXT> <POLICY STATEMENT COMMENTARY>In many systems, fixed passwords are the first and only line of defense. Although it's a long-established hacker technique, guessing fixed passwords remains a popular and often successful attack method by which unauthorized persons gain system access. In the past hackers used manual methods, but these days password guessing is most often performed with automated tools like dictionary attack programs (so-called 'crack' programs). For related comments, see the policies entitled "Anonymous User-IDs," "Limit On Consecutive Unsuccessful Attempts To Enter A Password," "Maximum Permissible Password Attempts For Dial-Up Users," "Disclosure Of Information In System Log-in Banner," and "Requirement For Different Passwords On Different Systems."</POLICY STATEMENT COMMENTARY> <POLICY STATEMENT EXAMPLE> After a certain number of days, the accounting system will require you to choose a new password. In order to maximize security, you will be required to use at least 8 characters. It is best not to use dictionary names or other easily-guessed words. /POLICY STATEMENT EXAMPLE> <POLICY STATEMENT RELATIONSHIP</p>

policyStatementIdentifier="CW PD USRIDANN/>

<POLICY STATEMENT RELATIONSHIP</p> policyStatementIdentifier="CW_PD_ATTEMPTLOGIN" />

<POLICY STATEMENT_RELATIONSHIP</pre> policyStatementIdentifier="CW_PD_LOGNPRELOGNBNNR" />

<POLICY STATEMENT RELATIONSHIP policyStatementIdentifier="CW PD USRIDANON" />

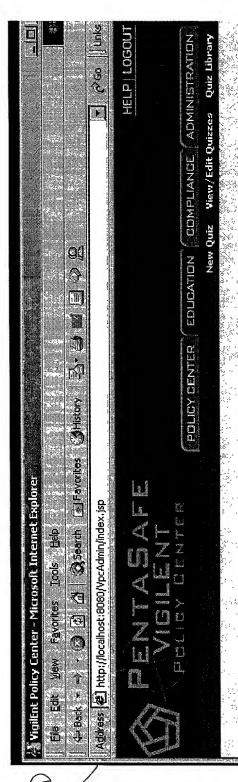
FIG. 6A

```
<POLICY ATTRIBUTE name="Audience">
           <POLICY ATTRIBUTE VALUE name="Technical" />
          !</POLICY ATTRIBUTE>
        I<POLICY ATTRIBUTE name="Environment">
           <POLICY ATTRIBUTE VALUE name="Low Security" />
           <POLICY_ATTRIBUTE_VALUE name="Medium Security" />
           <POLICY ATTRIBUTE VALUE name="High Security" />
          </POLICY ATTRIBUTE>
          <POLICY PARAMETER name="PSWRDMINLEN" type="characters"</p>
              value="8" />
              <PLATFORM ACTION platformType="AS400" title="Audit
                 Minimum Length of Passwords">
               > < PLATFORM ACTION TYPE>audit auto</PLATFORM ACT
                     ION TYPE>
                  <PLATFORM ACTION DESCRIPTION>For AS400 this audit
                     specifies the minimum number of characters in a password.
                     The risk is that passwords that are common names/words
                     are too short and/or have simple patterns are much easier to
                     guess and are therefore weak. If OPWDMINLEN is set to 4
                     or less, there is a greater chance that someone will guess the
                     password or watch a password being entered. The remedy is
                     that QPWDMINLEN should be set to 5 or
                     greater.</PLATFORM ACTION DESCRIPTION>
                 <ACTION PARAMETER name="GTSCMNPWDL"</p>
                     dataType="characters" classification="value" orderIndex="1"
                     score="10">
                 ACTION PARAMETER VALUE>8</ACTION PARAMETER
                   __YALUE>

∠ACTION PARAMETER>

          <u>{ </PL</u>ATFORM ACTION>
       !</POLICY_STATEMENT> /** End if Policy Statement **/
   </POLICY_CATEGORY> /** End of Policy Category **/
zo5b
  <SUPPORTED_LANGUAGE name="English" /> 228
</POLICY DOCUMENT> /** End of Policy Document **/
              2036
```

FIG. 6B



Policy Edioanion

Policy Center provides an easy way to educate your users on the currently published Security policies, and verify their knowledge through on-line tests. You can use one of our standard quizzes or create your own.



View/Edit Ouizzes gives you a quick overview of your current quiz documents and summary information for each. From there you can perform actions on each quiz, such as review, edit, copy or publish

<u>Ouiz Library gives you a quick overview of system quizzes and summary information for each From there</u> you can perform actions on each quiz, such as view or copy y

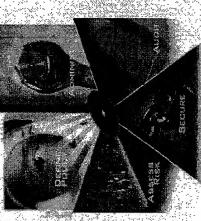


FIG. 7A

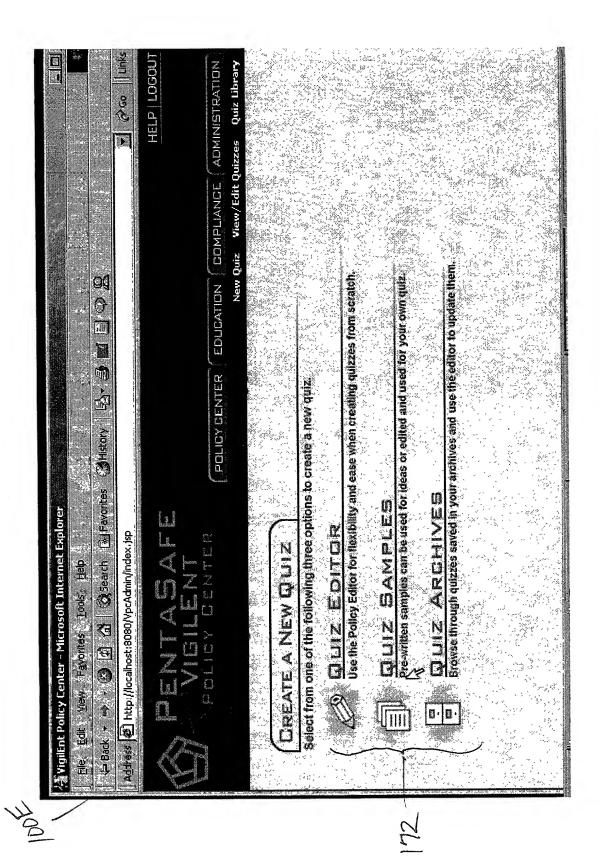


FIG. 7B

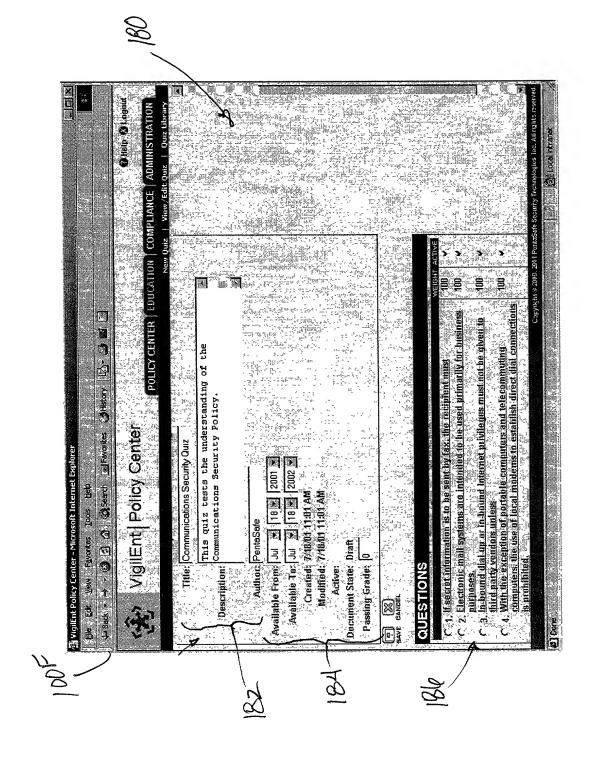
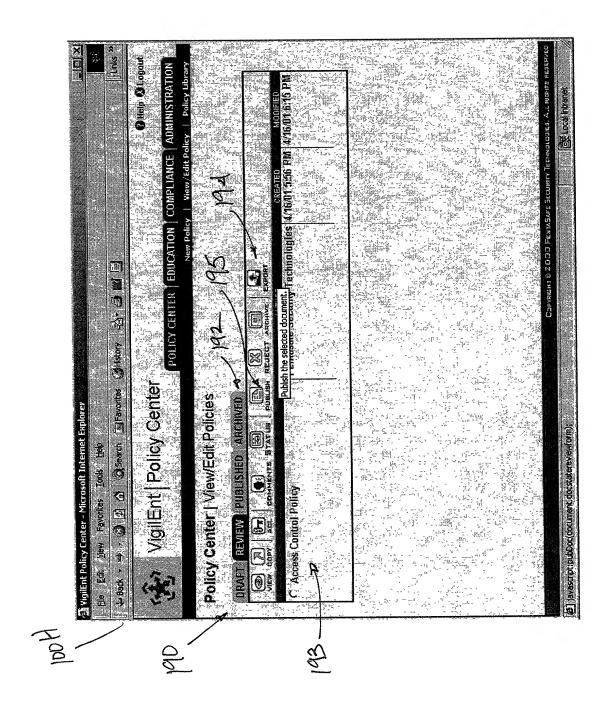


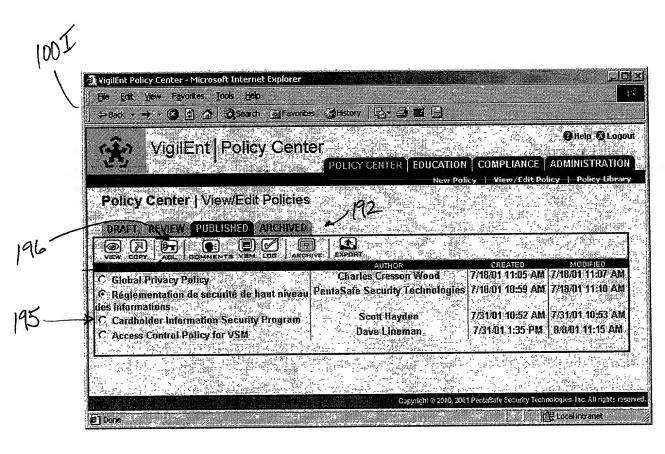
FIG. 7C

学Vigiliant Policy Center - Microsoft Internet Explorer. File Edit View Favorites Doy's 共中 File Edit View Favorites Doy's 共中 本語 Edit View Favorites	PELLICY CENTER POLICYCENTER EDUCATION DAMPLANDE ADMINISTRATION AUESTION Question Text. All users must be automatically forced to change their passwords at least once every ninety (p) days. Active: Weight Answer Text. Active: Weight Answer Text.
Wigilent Po	

FIG. 7D



FG. 8



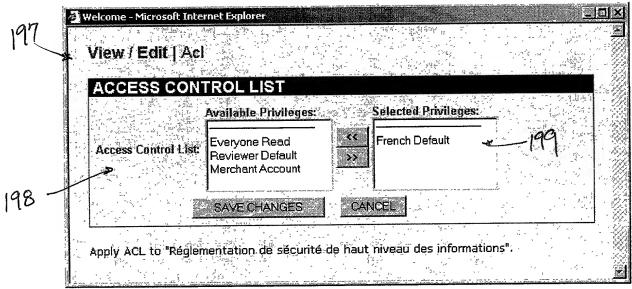


FIG. 9

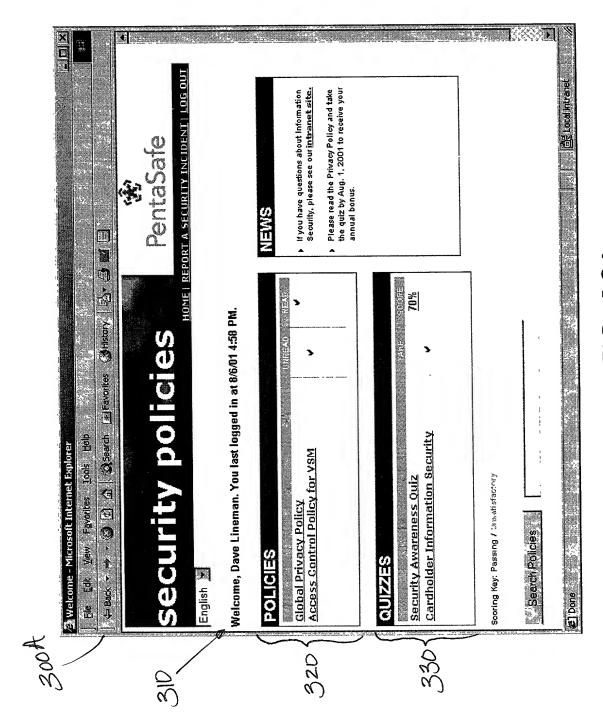


FIG. 10A

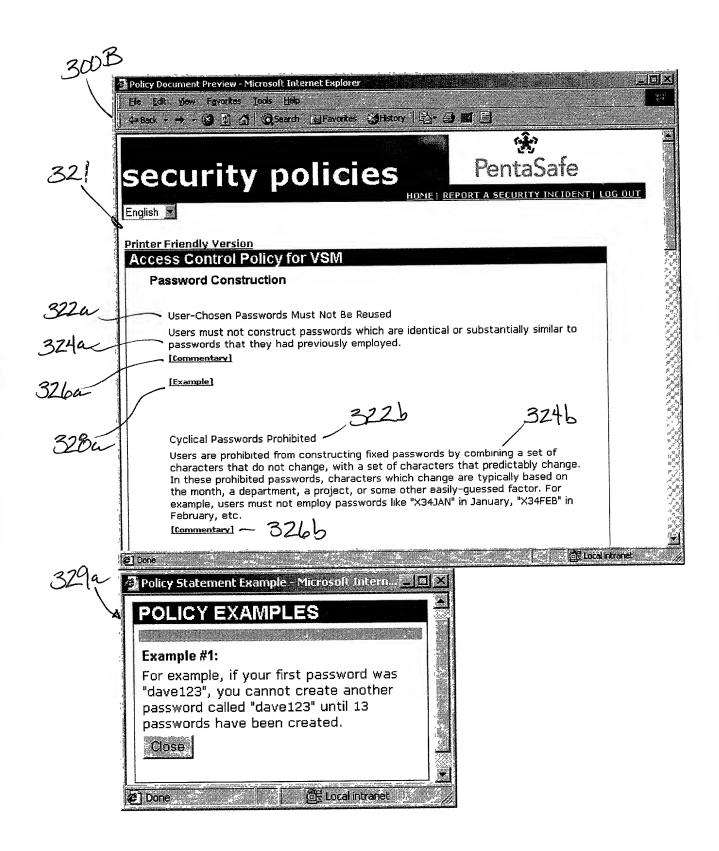


FIG. 10B

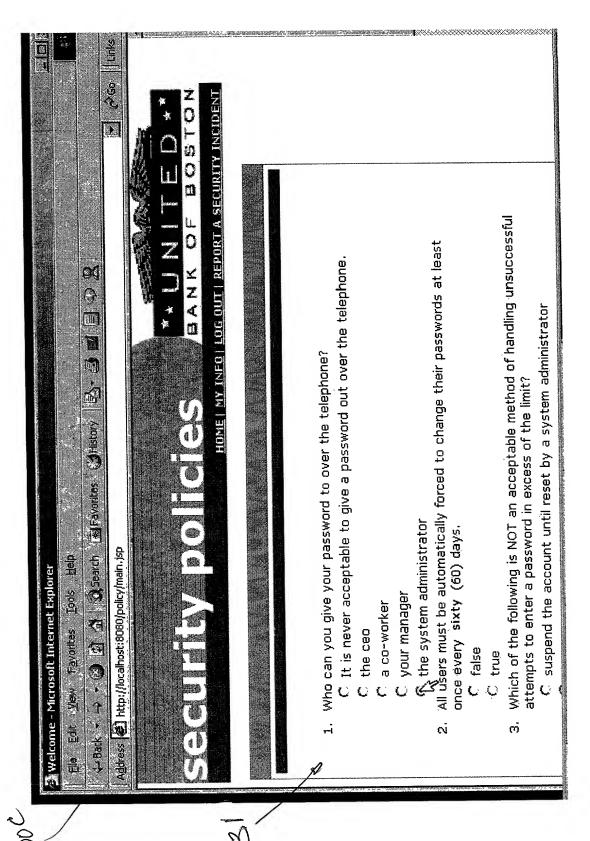
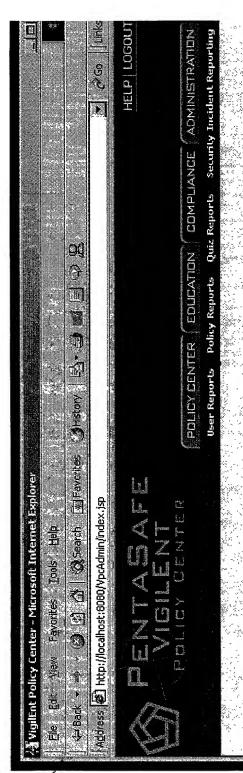


FIG. 10C



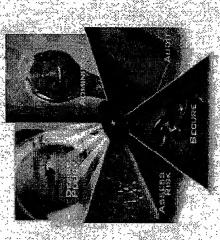
The Policy Compliance manager allows you to quickly verify which users in the organization have read and understood your published policies. You can also use this area to report and track security incidents.

<u>User Reports</u> allow you to track policy compliance by each user. You can either select individuals or groups of users and determine if they have read published policies or taken published quizzes.

<u>Policy, Reports</u> allow you to view compliance for a particular policy, documents



Security Incident Reporting allows you to report, manage and track security incidents in your enterprise. The incident reporting allows you to track critical details about your security incidents and produce





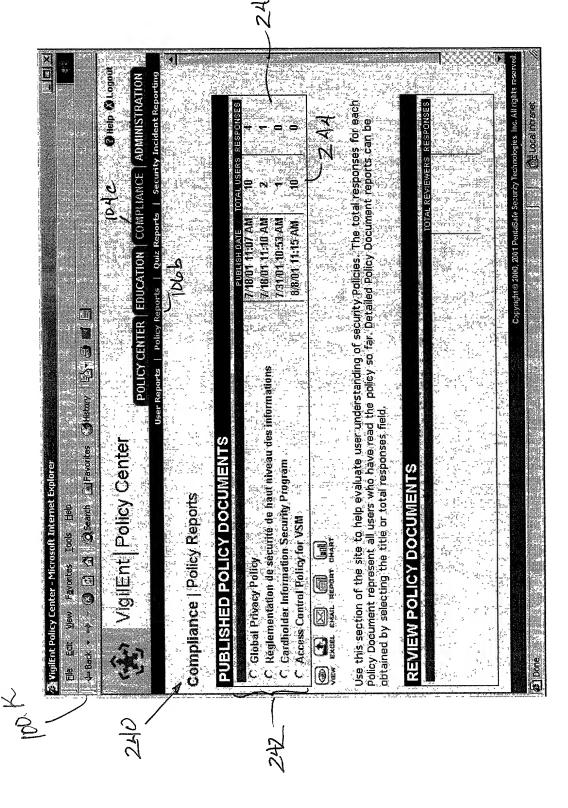


FIG. 11B

Compliance Policy Center Policy Reports Policy Reports Security Incident	File Edit Yew F	File Edit Yew Favorites" Loois Leb				
		2 2 Search	-avorites & History	8-9 1		
POLICY CENTER EDUCATION COMPLIANCE Des Reports Policy Reports Scott Savita Neddy Lineman 2001.07.16 2001.07.31 Powe e.acknowledged reading the policy document.						пØ фенØ
Policy Reports Policy Reports South Reddy Bob Jones Daye Lineman 2001-07-19 Eacknowledged, reading the policy, document.			100	CENTER EDUCATI	ON COMPLIANCE	
Policy Reports Scott Savita Bote Daye Lineman Lineman			User Reports	40.00 Vo		rity Incident Repo
ICV Policy IRST MANE South Savita Jones Jo		Policy Reports				
Cout Wellschem Savita Savita Jones Jave Lineman Lacknowledged reading the policy do		cy Policy				
Savita 30tr 30tr 30tr 30tr 30tr 30tr 30tr 30tr		Alwer -		07.18		
Jave Lineman Laman Acknowledged reading the policy do						
Expension of the policy document. These users have acknowledged reading the policy document.						
These users have acknowledged reading the policy document.						
Excellence in the policy document. These users have acknowledged reading the policy document.						
These users have acknowledged reading the policy document.						
	These users have	acknowledged reading	the policy docume			

FIG. 11C

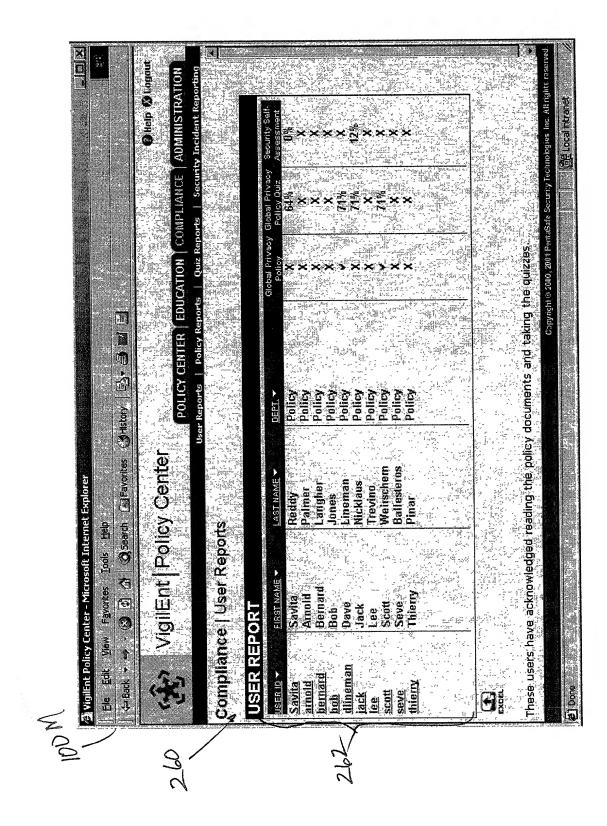


FIG. 11D

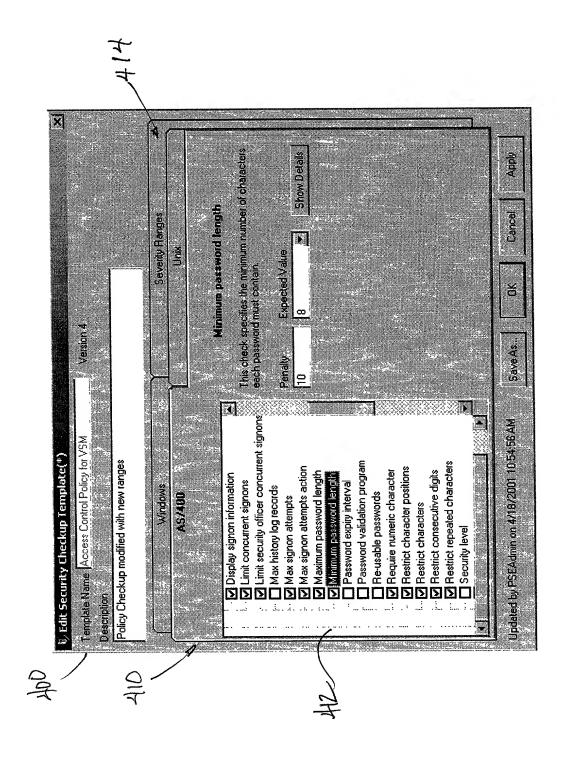


FIG. 12

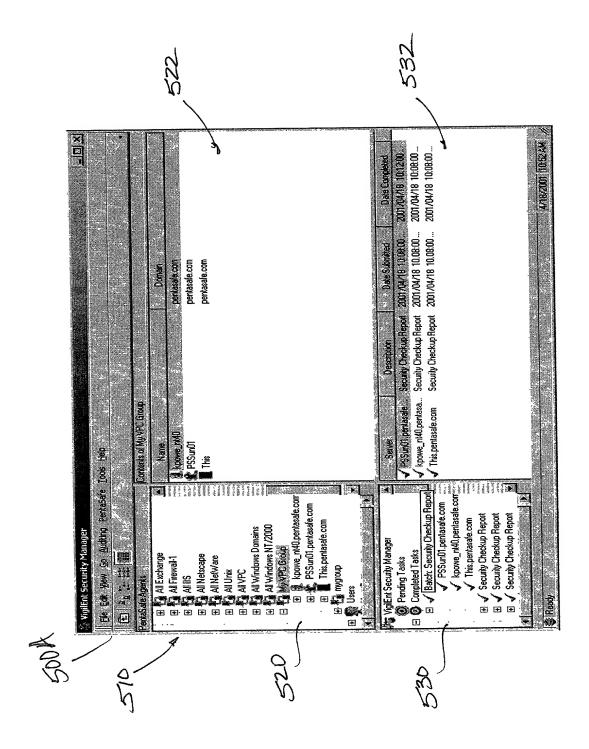


FIG. 13A

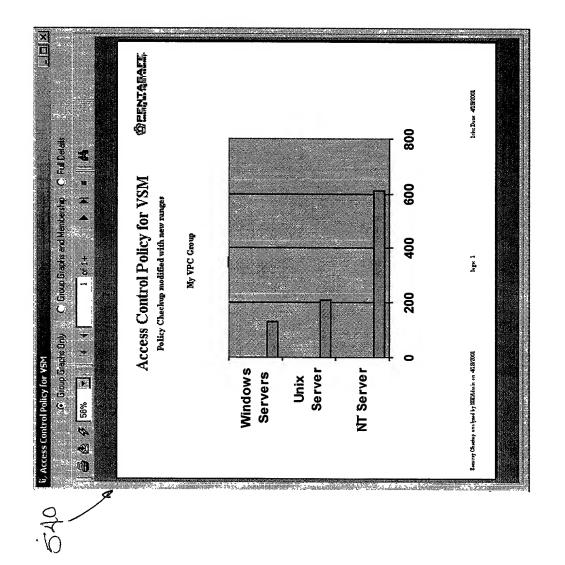
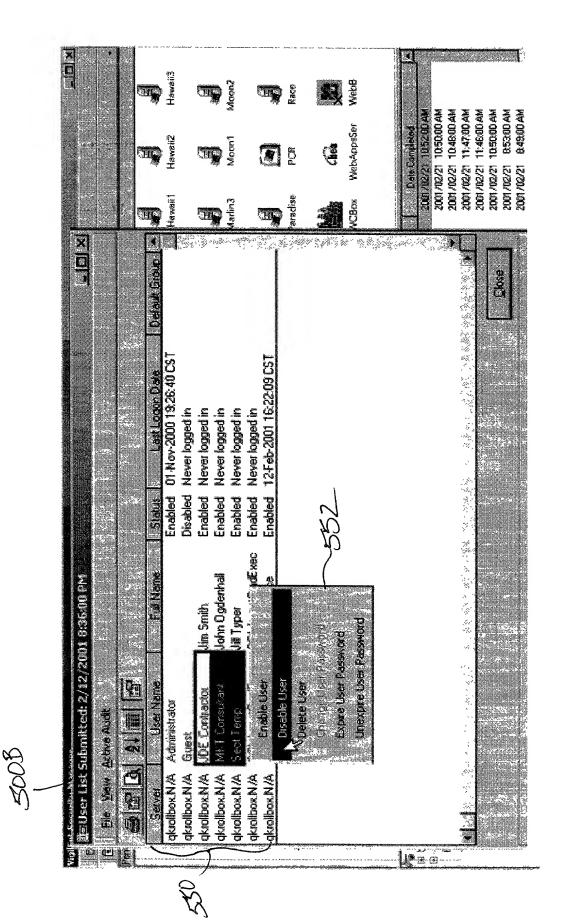


FIG. 13B



FIG, 13C

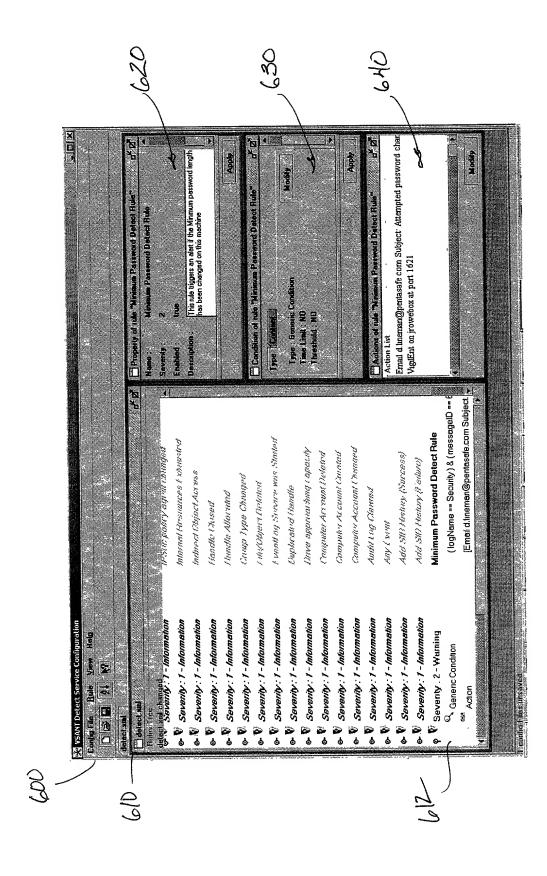


FIG. 14